Cyclotomic Coefficients: A Geometric Approach

Jakob Schneider, Frederik Benzing
MPIM Bonn

September 15, 2012

Abstract

This paper is intended to be helpful for interested number theorists in finding new ideas of proving upper (or lower) bounds for the k-th coefficient of pqrth cyclotomic polynomial where $2 < p < q < r$ are primes. This coefficient is denoted by $a_{pqr}(k)$ and the bounds we search are functions of p and k. Now, during our considerations of the problem just mentioned, we drew the conclusion that these bounds can probably be found using a more geometric interpretation than classic means of number theory.

On the other hand, with these methods we cannot directly get results about the original problem, but we are sure that there is a way to rebridge this gap between geometric arguments and discrete numbers.

So this paper is dedicated to everyone who wants to prove bounds for $a_{pqr}(k)$ and has no idea about there formulae, because the things that are worked out in the next pages lead to an amazing generalization of the proven fact that $a_{pqr}(k) \leq 2/3p$.

1 Introduction

To see how to arrive at the geometric problem we may start from the following lemma by Kaplan:

Lemma 1. *For $n \in \mathbb{Z}$ denote by $[n]_p$ and $[n]_q$ the unique integers $\alpha \in \{0, \dots, q-1\}$ and $\beta \in \{0, \dots, p-1\}$, respectively, such that $n \equiv \alpha p + \beta q \pmod{pq}$. Then we define*

$$b_i^k := \begin{cases} 1 & : [i]_p < [1]_p \wedge [i]_q < [1]_q \wedge i \leq k/r \\ -1 & : [i]_p \geq [1]_p \wedge [i]_q \geq [1]_q \wedge i \leq k/r + pq \\ 0 & : \textit{otherwise} \end{cases} \tag{1}$$

Furthermore, define $f(m)$ to be the unique integer such that $f(m) \equiv r^{-1}(k-m) \pmod{pq}$ and $f(m) \in \{0, \dots, pq-1\}$. Then we have

$$a_{pqr}(k) = \sum_{m=0}^{p-1} \left(b_{f(m)}^k - b_{f(m+q)}^k \right). \tag{2}$$

Considering this lemma, we can find a geometric interpretation of all these variables (namely the one introduced by Dominik Duda). We just have to define the map

$$\boldsymbol{v} : \{0, \dots, pq-1\} \to [0,1)^2, \text{ where } n \mapsto \left(\frac{[n]_p}{q}, \frac{[n]_q}{p} \right). \tag{3}$$

In fact, $\boldsymbol{v}$ is a linear function modulo 1. Now for an easier representation of the variables we introduce the following definitions:

$$s := \frac{k}{pqr}, \qquad \sigma := \frac{[1]_q}{p}, \qquad \rho := 1 - \sigma \qquad \text{and} \tag{4}$$

$$\boldsymbol{m} := \boldsymbol{v}(f(1) - f(0)), \qquad \boldsymbol{n} := \boldsymbol{v}(f(0)), \qquad \boldsymbol{d} := \boldsymbol{v}(f(q) - f(0)). \tag{5}$$

We then have that $s \in \frac{\mathbb{Z}_{pqr}}{pqr} \cap [0,1]$ (since we set $k < pqr$), $\sigma, \rho \in \frac{\mathbb{Z}_p^\times}{p} \cap [0,1]$, $\boldsymbol{m}, \boldsymbol{n} \in \frac{\mathbb{Z}_q^\times}{q} \times \frac{\mathbb{Z}_p^\times}{p}$ and $\boldsymbol{d} \in \{0\} \times \frac{\mathbb{Z}_p^\times}{p}$. Define the polygonal sets:

$$F^+ := \{(x,y) \in \mathbb{R}^2 : 0 \le x < \rho \wedge 0 \le y < \sigma \wedge x + y \le s\} + \mathbb{Z}^2, \tag{6}$$

$$F^- := \{(x,y) \in \mathbb{R}^2 : \rho \le x < 1 \wedge \sigma \le y < 1 \wedge x + y \le s + 1\} + \mathbb{Z}^2. \tag{7}$$

Then we may reformulate the lemma as follows (as done by Dominik Duda):

Lemma 2. *Let $\{\boldsymbol{a}_i\}_{i=0}^{p-1}$ and $\{\boldsymbol{b}_i\}_{i=0}^{p-1}$ sequences in $\mathbb{R}^2$ where $\boldsymbol{a}_i := \boldsymbol{m}i + \boldsymbol{n}$ and $\boldsymbol{b}_i := \boldsymbol{a}_i + \boldsymbol{d}$, respectively. Then we have*

$$a_{pqr}(k) = |F^+ \cap \{\boldsymbol{a}_i\}_{i=0}^{p-1}| - |F^- \cap \{\boldsymbol{a}_i\}_{i=0}^{p-1}| - |F^+ \cap \{\boldsymbol{b}_i\}_{i=0}^{p-1}| + |F^- \cap \{\boldsymbol{b}_i\}_{i=0}^{p-1}|. \tag{8}$$

In fact, this is just a geometric view of the things, but gives a better impression of the problem. Now we forget every number theoretical aspect behind these variables $s, \sigma, \rho, \boldsymbol{m}, \boldsymbol{n}, \boldsymbol{d}$ and just consider the problem as a geometric one. This means, we ignore the constraints on them given by their definition and just care for the sets they belong to and some other proporties of the original problem.

2 Weaker Formulations

Now, we formulate two versions of the corresponding geometric problem invoking no number theoretical background. Indeed, it then suggests the idea of finding bounds for the general geometric problem which then should be pretty sharp bounds for $|a_{pqr}(k)|$ ($q, r \in \mathbb{P}$, $k \in \mathbb{Z}$).

The Geometric Problem V1 & V2. We now formulate the geometric Problem using no number theoretical background:

Definition. Given a $p \in \mathbb{Z}^+$ (not necessarily a prime). Then we define

$$\mathcal{C}_p := \left\{ (s, \rho, \sigma) \in [0,1) \times \left(\frac{\mathbb{Z}_p^\times}{p} \right)^2 : \rho + \sigma = 1 \right\}, \tag{9}$$

$$\tilde{\mathcal{C}}_{(p)} := \{(s, \rho, \sigma) \in [0,1)^3 : \rho + \sigma = 1\} \tag{10}$$

and

$$\mathcal{S}_p := \left\{ (\boldsymbol{m}, \boldsymbol{n}, \boldsymbol{d}) \in \left(\mathbb{R} \times \frac{\mathbb{Z}_p^\times}{p} \right)^2 \times \left(\{0\} \times \frac{\mathbb{Z}_p^\times}{p} \right) \right\}, \tag{11}$$

$$\tilde{\mathcal{S}}_p := \left\{ (\boldsymbol{m}, \boldsymbol{n}, \boldsymbol{d}) \in \left(\mathbb{R} \times \left(\left[\frac{1}{p}, \frac{p-1}{p} \right] + \mathbb{Z} \right) \right) \times \mathbb{R}^2 \times (\{0\} \times \mathbb{R}) \right\}. \tag{12}$$

Then for $(C, S) \in \mathcal{C}_p \times \mathcal{S}_p$ define $F^+(C)$ and $F^-(C)$ as in (6) and (7) $\{\boldsymbol{a}_i(S)\}_{i=0}^{p-1}$ and $\{\boldsymbol{b}_i(S)\}_{i=0}^{p-1}$ as in Lemma 2. And the do the same with tildes over all variables.

Now, define functions from $\tilde{\mathcal{C}}_{(p)} \times \tilde{\mathcal{S}}_p$ (and thus from $\mathcal{C}_p \times \mathcal{S}_p$) to $\mathbb{R}$:

$$p_1^+(C,S) := |F^+(C) \cap \{\boldsymbol{a}_i(S)\}_{i=0}^{p-1}|, \tag{13}$$
$$p_1^-(C,S) := |F^-(C) \cap \{\boldsymbol{a}_i(S)\}_{i=0}^{p-1}|, \tag{14}$$
$$p_2^+(C,S) := |F^+(C) \cap \{\boldsymbol{b}_i(S)\}_{i=0}^{p-1}|, \tag{15}$$
$$p_2^-(C,S) := |F^-(C) \cap \{\boldsymbol{b}_i(S)\}_{i=0}^{p-1}|, \tag{16}$$
$$p_1(C,S) := p_1^+(C,S) - p_1^-(C,S), \tag{17}$$
$$p_2(C,S) := p_2^-(C,S) - p_2^+(C,S), \tag{18}$$
$$p(C,S) := p_1(C,S) + p_2(C,S). \tag{19}$$

In the following consideration we often drop the (C,S) behind the functions and the other objects.

Reconsideration. Now we want to find an upper bounds $B_1(p)$ and $B_2(p)$, such that

$$\max_{(C,S)\in\mathcal{C}_p\times\mathcal{S}_p}\{|p(C,S)|\} =: M_1(p) \leq B_1(p), \max_{(C,S)\in\tilde{\mathcal{C}}\times\tilde{\mathcal{S}}_p}\{|p(C,S)|\} =: M_2(p) \leq B_2(p). \tag{20}$$

On the other hand, due to corrected Beiter conjecture it is straight forward to claim that for p large enough $B_1(p) := B_2(p) := 2/3p + C$ is a possible bound (for some constant $C \in \mathbb{R}^+$).

Remark. We may say that there are no points of $\{\boldsymbol{a}_i\}_{i=0}^{p-1}$ or $\{\boldsymbol{b}_i\}_{i=0}^{p-1}$ lying on the boundaries of F^+ or F^- that incident with $\{(x,y) \in \mathbb{R}^2 : x + y = s\} + \mathbb{Z}^2$. This is because we then can change s by $\varepsilon > 0$ (increase or decrease) such that the newly build C' satisfies $p(C,S) = p(C',S)$ and there are no points of the two sequences on those boundaries of F'^+ and F'^-, respectively. Analogously, we infer that we may assume that there are no points of the sequences $\{\boldsymbol{a}_i\}_{i=0}^{p-1}$ or $\{\boldsymbol{b}_i\}_{i=0}^{p-1}$ on all closed boundaries of F^+ or F^- (this time we have to manipulate s and $\{\boldsymbol{a}_i\}_{i=0}^{p-1}$, $\{\boldsymbol{b}_i\}_{i=0}^{p-1}$ a little).

Now we denote by $\mathcal{G}_p \subset \mathcal{C}_p \times \mathcal{S}_p$ (and $\tilde{\mathcal{G}}_p \subset \tilde{\mathcal{C}}_{(p)} \times \tilde{\mathcal{S}}_p$) all these 'non degenerated' pairs of $(C,S) \in \mathcal{C}_p \times \mathcal{S}_p$ (and $(C,S) \in \tilde{\mathcal{C}}_(p) \times \tilde{\mathcal{S}}_p$), i.e. there are no points of the sequences lying on closed boundaries of the sets F^+ and F^- (or $\tilde{F}^+$ and $\tilde{F}^-$).

3 Symmetries of The Construction

The first thing we want to deal with is some symmetry properties of the newly build problems. The first one is formulated in the following

Lemma 3. *Let $(C,S) = ((s,\rho,\sigma),(\boldsymbol{m},\boldsymbol{n},\boldsymbol{d})) \in \tilde{\mathcal{G}}_p$ be a constellation. Then the following identities hold.*

(i) For $C_1 = (1-s,\rho,\sigma)$ we have $p(C_1,S) = p(C,S)$.

(ii) Setting $C_2 = (s,\sigma,\rho)$, it holds that $p(C_2,S) = p(C,S)$.

(iii) Defining $S_1 = (\boldsymbol{m},\boldsymbol{n},-\boldsymbol{d})$, we obtain $p(C,S_1) = -p(C,S)$.

(iv) For $C_3 = (s,d_2,\sigma)$ and $S_2 = (\boldsymbol{m},\boldsymbol{n},.)$, we have that $p(C_3,S_2) = p(C,S)$.....